REMARKS

This Amendment responds to the Office Action mailed April 6, 2007 in the above-identified application. Based on the foregoing amendments and the following comments, reconsideration and allowance of the application are respectfully requested.

Claims 1-6, 9-12, 17 and 18 were previously pending in the application. By this Amendment, independent claims 1, 4, 6, 12 and 18 have been amended. Claims 3, 5, 9 and 10 have been canceled without prejudice or disclaimer. Accordingly, claims 1, 2, 4, 6, 11, 12, 17 and 18 are currently pending. The amendments find clear support in the original application at least at page 7, lines 5-16 and Fig. 4C. No new matter has been added.

The Examiner has rejected claims 1-6, 9-12 and 17-18 under 35 U.S.C. §103(a) as unpatentable over Sato et al. (US 5,734,855) in view of Philipp (DE 19936890). The rejection is respectfully traversed in view of the amended claims.

Sato discloses a data processor in which a temporary register is used to store the result of an operation before the result is transferred to a destination register. (Fig. 2 and col. 2, lines 14-57). However, Sato does not disclose storing a random number in the destination register for masking the operation.

Philipp discloses a cryptographic operation which provides for a data bit word generated on the basis of random numbers to be stored in a memory cell or a register before a data bit word is written into the same (Abstract).

Amended claim 1 is directed to an integrated circuit implementing at least one operator involving at least one secret quantity, and functionally comprising upstream and downstream of the operator at least first and second source registers and at least one destination register, respectively, at least one temporary register, means for loading a first random or pseudo-random number into the temporary register, means for transferring the content of the first source register into the temporary register, and means for loading a second random or pseudo-random number into the destination register, the operator combining the content of the second source register and the temporary register and storing the result in the destination register.

Sato and Philipp, taken individually or in combination, do not disclose or suggest an integrated circuit as defined by amended claim 1. In particular, Sato and Philipp do not disclose or suggest loading a first random or pseudo-random number into a temporary register,

transferring the content of the first source register to the temporary register, loading a second random or pseudo-random number into the destination register, the operator combining the content of the second source register and the temporary register and storing the result in the destination register. For these reasons, amended claim 1 is clearly and patentably distinguished over Sato in view of Philipp, and withdrawal of the rejection is respectfully requested.

Claim 2 depends from claim 1 and is patentable over the cited references for at least the same reasons as claim 1.

Amended claim 4 is directed to an antifraud method comprising randomizing a content of a destination register of a result of an operator involving at least one secret quantity. Amended claim 4 contains method limitations that parallel the apparatus limitations of claim 1. Amended claim 4 is patentable over Sato in view of Philipp for at least the same reasons as claim 1.

Amended claim 6 is directed to an integrated circuit and contains limitations that parallel the limitations of amended claim 1. Claim 6 is patentable over Sato in view of Philipp for at least the same reasons as claim 1.

Claim 11 depends from claim 6 and is patentable over the cited references for at least the same reasons as claim 6.

Amended claim 12 is directed to an antifraud method and contains method limitations that parallel the apparatus limitations of amended claim 1. Claim 12 is patentable over Sato in view of Philipp for at least the same reasons as claim 1.

Claim 17 depends from claim 12 and is patentable over the cited references for at least the same reasons as claim 12.

Amended claim 18 is directed to an antifraud method and contains method limitations that parallel the limitations of claims 1, 4, 6 and 12. Claim 18 is patentable over Sato in view of Philipp for at least the same reasons as claim 1.

Based upon the above discussion, claims 1, 2, 4, 6, 11, 12, 17 and 18 are in condition for allowance.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: July 5, 2007

Respectfully submitted,

By: William R. McClellan

William R. McClellan
Registration No.: 29,409
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000

DD: 07/06/07